

UNITED STATES DISTRICT COURT

for the  
District of Oregon

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

A blue Samsung Galaxy S9 currently located on the premises of the Federal  
Bureau of Investigation, Secure Evidence Storage, item 1B7, in Eugene,  
Oregon, as further described in Attachment A

Case No. 6:22-mc-1024

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

A blue Samsung Galaxy S9 currently located on the premises of the Federal Bureau of Investigation, Secure Evidence Storage, item 1B7, in Eugene, Oregon, as further described in Attachment A  
located in the \_\_\_\_\_ District of \_\_\_\_\_ Oregon \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252A(a)(1), (a)(2) and (a)(5)(B)	Possession, receipt, and distribution of visual depictions of minors engaged in sexually explicit conduct and/or child pornography.

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Deane Davis, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

Telephone at 4:45pm a.m./p.m. (specify reliable electronic means).

Date: October 28, 2022

City and state: Eugene, Oregon

  
Judge's signature

Mustafa T. Kasubhai, United States Magistrate Judge

Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF DEANE RAWLINSON DAVIS

**Affidavit in Support of an Application  
Under Rule 41 for a Search Warrant**

I, Deane Rawlinson Davis, being duly sworn, do hereby depose and state as follows:

**Introduction and Agent Background**

1. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed since 2021. I am currently assigned to the Eugene Resident Agency (EURA). In this position I am tasked with investigating federal crimes within EURA's area of responsibility, to include child exploitation and possession, distribution, and production of child pornography. Prior to my employment with the FBI, I was a sworn law enforcement officer employed by the Washington State Liquor and Cannabis Board (WSLCB) from 2017-2021. I have completed training at the FBI Academy at Quantico, Virginia and the Washington State Criminal Justice Training Commission – Basic Law Enforcement Academy. For most of my employment with WSLCB I was assigned to the Marijuana Enforcement Unit, where I was tasked with investigating criminal and administrative violations with a nexus to marijuana in Washington State. I have received additional training in Criminal Investigations, Interdiction Operations, Cell Phone, Social Media and Digital Investigations, and am a certified NIK Polytesting Drug Identification Instructor/Trainer. In my official law enforcement duties, I have written and participated in the execution of search warrants, both for physical locations and electronic data. I am currently a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of a

blue Samsung Galaxy S9, FCCID #A3LSMG96OU (hereinafter “the Subject Phone”), currently in law enforcement’s possession at the Eugene, Oregon office of the FBI. The Phone has been securely in FBI possession since it was seized by law enforcement on June 11, 2021. As set forth below, I submit that probable cause exists to believe and I do believe that the items set forth in Attachment B constitute evidence of violations of Title 18, United States Code (U.S.C.), Sections 2252A(a)(2), (b)(1) and 2252A(a)(5)(B) and (b)(2).

3. This affidavit is intended to show only that sufficient probable cause exists for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

#### **Applicable Law**

4. As set forth below, I submit that probable cause exists to believe, and I do believe, that the Subject Phone contains evidence of the following violations:

**Title 18 U.S.C. § 2252A(a)(2) and (a)(5) and (b)(1) (Receipt and Possession of Child Pornography)** provides in part, that whoever, knowingly receives any child pornography that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempts to do so, shall be

fined and imprisoned not less than 5 years and not more than 20 years (for receipt, there is not mandatory minimum sentence for possession).

### **Statement of Probable Cause<sup>1</sup>**

#### **Summary**

5. Law enforcement identified accounts belonging to a suspected distributor of child pornography in 2020. In 2021, the investigation of those accounts led to the identification of a premises as well as a suspected user of those accounts, Randy L. Cook. Accordingly, the FBI sought and obtained a search warrant for Cook's geolocation information as well as a warrant for that premises, a vehicle, and Cook's person. On June 11, 2021, the day that warrant was executed, law enforcement contacted Cook away from his residence driving a vehicle that was not included in the search warrant. Law enforcement learned that Cook left two cellular

---

<sup>1</sup> Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *IP address.* The Internet Protocol address (or simply "IP address") is a unique numeric address used by digital devices on the Internet. Every digital device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that digital device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some digital devices have static—that is, long-term—IP addresses, while other digital devices have dynamic—that is, frequently changed—IP addresses.

b. *Internet.* The Internet is a global network of digital devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. *Storage medium.* A storage medium is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

devices, including the Subject Phone, in that vehicle and seized them pursuant to the automobile exception. Both phones were lodged as evidence in FBI custody. This application seeks authorization to search the Subject Phone.

### **Initial Undercover Investigation and Identification of Cook**

6. An FBI online undercover investigation discovered that a suspect in a New York investigation, referred to herein as Suspect 1 (S1) was an administrator of a Kik group engaged in exchanging child pornography. In July 2020, the NY Division of the FBI executed a search warrant at S1's residence. S1's phones were seized, and child pornography was discovered along with Kik chats. Upon review of the Kik chats, FBI NY Division identified the user "itssmalldontworry / J Macky", as a member of a Kik Group engaged in the exchange of child sex abuse material (CSAM), which includes child pornography. The Kik Group, entitled "Hot Group", exchanged sexually explicit files of males aged 6 to 16 years, nude or engaged in sexual activity. On 06/30/2020, "itssmalldontworry" contacted S1 on Kik, and stated, "34 m. Any age bit favorite is between 7 and 14". "itssmalldontworry" sent S1 images of CSAM which constitute child pornography, two of which are detailed below:

- The first image depicts a prepubescent male's erect penis with a substance that appears to be semen.
- The second image depicts a prepubescent male pulling his legs back to expose his anus and penis.

S1, an administrator of multiple Kik groups, then informed "itssmalldontworry" that he would add him to one of the Kik Groups entitled "#boylust". Shortly after, it appears that

"itssmalldontworry" accessed the Kik Group identified as "Hot Group". While "itssmalldontworry" did not send any child pornography to the group, multiple members of the group posted child pornography for the group to view.

7. On August 19, 2020, results of a subpoena served to Kik for "itssmalldontworry" provided the following information:

- Name: J Macky
- Email: jmack198585@gmail.com
- Login IP: 47.33.137.221 (Spectrum/Charter)
- Registration Device: Android LGL722DL
- Registration Date: May 28, 2020

8. Open-source search for an Android LGL722DL yielded the device is likely a Tracfone. Based on my training and experience, I know that cellular phones are often kept on a person and in their direct control.

9. On April 2, 2021, results of a subpoena served to Google for the email used to register the subject Kik account, "jmack198585@gmail.com," provided the following information:

- Name: Jerry Mack
- Registration IP: 174.253.214.66 (Verizon Wireless)
- Registration Date: May 28, 2020

Based on my training and experience, I know that users often set up fake email accounts to link to messaging accounts to maintain anonymity. Given that the above Gmail account was registered on the same date as the subject Kik account—May 28, 2020—this Gmail account is likely an account created for anonymity, often referred to as a “spoof” account.

10. On September 8, 2020, results of a subpoena served to Spectrum/Charter for the IP Address associated with the subject Kik account provided the following information:

- Subscriber: Randy Cook
- Address: 37707 Camp Creek Rd Springfield, OR 97478
- Phone: (541) 632-0803
- MAC: C8B4225F8AA7

11. On October 1, 2020, a search for individuals residing at 37707 Camp Creek Road, Springfield, Oregon identified Randy Lee Cook, DOB XX/XX/1980. These checks also indicated Cook is a registered sex offender. Criminal history checks for Cook identified a 2006 arrest in Missouri for Promoting the Sexual Performance of a Child. Law enforcement reviewed the probable cause affidavit for that matter, and it reflects that Cook engaged in sexually explicit online chats with an underage minor female, as well as sending sexually explicit images of himself and other minor children. Cook was charged by the McDonald County Sheriff's Office for 1<sup>st</sup> Degree Promoting Child Pornography, found guilty, and sentenced to twelve years in prison.

12. An open source search yielded Facebook profile "Randy C". Search of publicly available content on that profile showed multiple images of trucks and references the business RLC Trucking LLC. Additional open source searches for Randy Lee Cook yielded positive results for the owner of RLC Trucking, LLC which is registered at 2753 Maia Loop, Springfield, Oregon 97477. Facebook page for "RLC Trucking" promotes a log truck business.

13. An open source search for telephone number 541-632-0803 yielded a linked Skype account with username "r.c.1822" and display name "Randy C". Search for username

"itssmalldontworry" yielded previously identified Kik account with username "J Macky".

14. On November 13, 2020, an FBI online undercover identified Kik user "itssmalldontworry / J Macky" posted six images and one video of child pornography in Kik group "Boys For Play". The images were of prepubescent boys nude and/or in sexual acts.

15. On February 18, 2021, a Sex Offender Registry Check with Oregon State Police Sex Offender Registration Section confirmed that Cook is a registered sex offender with the following information provided by Cook on June 16, 2020:

- Address: 37707 Camp Creek Rd Springfield, OR 97478
- Phone: (541) 632-0803
- Occupation: Self Employed Truck Driver
- Vehicle: 1997 Red Ford F350 Crew Cab, OR License Plate YQJ896

16. On February 19, 2021, results of a subpoena served to Verizon for the aforementioned telephone number 541-632-0803 (associated with Cook) provided the following relevant information:

- Subscriber: Adult Witness 1
- Address: 37707 Camp Creek Rd., Springfield OR
- Effective Date: 02/27/2014
- Status: Active

17. On March 4, 2021, law enforcement conducted surveillance at 37707 Camp Creek Rd, Springfield Oregon. During the surveillance, a WiFi survey was completed, which captured two "encrypted" or secured networks, within approximately 275 feet of subject Premises, with the following MAC addresses:

- **SSID:** MySpectrumWiFiA7-2G **MAC:** C8:B4:22:5F:8A:A5



- **SSID:** MySpectrumWiFiA7-5G **MAC:** C8:B4:22:5F:8A:A6

The MAC address provided for Cook by Charter Communications, C8B4225F8AA7 (previously documented in Paragraph 10), is almost an exact match. Based on open source information, as well as conversations with other law enforcement personnel, when only the last digits of a MAC address are different, it is indicative of a WiFi Access Point (AP)/router that serves different frequencies, such as 2.4Ghz and 5Ghz. The Charter Communications MAC address ending in “A7” is likely another interface on the router, possibly the Ethernet port used to plug in a physical cable. Based on this information, it is likely that all of these MAC addresses are from the same device.

18. On April 27, 2021, and again on May 28, 2021, the Honorable Mustafa T. Kasubhai signed a search warrant and extension authorizing collection of the geolocation information for the above telephone number associated with the IP Address assigned to the Kik account for “itsmalldontworry,” which law enforcement believed belonged to Cook, and which law enforcement believed to contain evidence of the above Offenses. Geolocation information corroborated that the user of the cell phone was likely residing in the area of 37707 Camp Creek Rd, Springfield OR, Cook’s known residence.

#### **Additional CyberTipline Reports Obtained**

19. On July 14, 2021, law enforcement received information from the Crimes Against Children and Human Trafficking Unit, FBI HQ, that a user with a Kik account, likely registered sex offender Randy Lee Cook, was involved in the transmission and possession of child pornography, as detailed below.

20. On March 22, 2021, Kik submitted CyberTipline Report 87946561 to the National Center for Missing and Exploited Children (NCMEC). The report identified nine images and 17 videos depicting suspected child pornography being uploaded to a Kik account between 3/8/21 and 3/10/21, with the following user credentials:

- Email: jerrsmith1985@gmail.com
- Screen/User Name: doessizemater
- ESP User ID: doessizemater\_f9u
- Kik Upload IPs: 174.214.28.115 on 3/10/21; 174.214.29.5 on 3/9/21;

174.253.193.82 on 3/8/21.

Law enforcement noted the similarity of the username associated with this Kik account—“doessizemater”—to the username associated with the above-identified Kik account from the FBI undercover investigation—“itsmalldontworry” and believes both Kik usernames include references to the size of genitalia and related sexual innuendo.

21. On or about April 23, 2021, results of a subpoena served to Google for “jerrsmith1985@gmail.com” identified no records.

22. On or about April 27, 2021, results of a subpoena served to Verizon Wireless pertaining to Kik Upload IPs identified 701-818-4646 as the only unique telephone number associated with all login dates.

23. On or about May 3, 2021, results of a subpoena served to Verizon Wireless to provide information pertaining to telephone number 701-818-4646 yielded the following subscriber information:

- Start Date: 2/19/21
- Business Name/Reseller: TracFone

24. On or about May 7, 2021, results of a subpoena served to Kik for "doessizemater" provided the following additional information:

- Name: J Smith
- Email: jerrsmith1985@gmail.com (unconfirmed)
- Login IPs: 47.33.137.132 (PORT 53434 on 3/30/21); 47.33.137.132 (PORT 40022 on 2/25/21) (Spectrum/Charter Communications)
- Registration Device: Android LGL722DL
- Registration Date: February 19, 2021

25. On or about May 17, 2021, results of a subpoena served to Charter Communications for information pertaining to Kik Login IPs 47.33.137.132 on 2/25/21 at 10:06:25AM UTC PORT 40022 and on 3/30/21 at 12:00:52AM UTC PORT 53434 provided the following:

- Subscriber Name: Randy Cook
- Service Address: 37707 Camp Creek Rd, Springfield, OR 97478
- User Name: krausch04@charter.net
- Phone Number: 5416320803
- Account Number: 8751141100134689
- MAC: C8B4225F8AA7
- Start Date: 9/14/2020

26. On or about May 27, 2021, results of a subpoena served to TracFone Wireless, Inc. for information pertaining to telephone number 701-818-4646 provided mostly incomplete/unidentifiable subscriber information, with an activation date of 2/19/21 and a deactivation date of 5/23/21.

27. On July 23, 2021, law enforcement reviewed the images/videos provided to NCMEC by Kik via CyberTipline Report 87946561, two examples of which are described below.

28. The first example, a one minute and 53-second video (file: f-446813-c149-4fc2-9810-952762ce6964.mp4), depicts two female girls, estimated to be between four to six years old. Both girls are completely nude. One girl, blonde with ponytails in her hair, is laying on her back with her legs spread and knees bent, exposing her vaginal area. The second child, a brunette, is laying on her stomach with her mouth and finger inside the other child's vagina, performing oral sex on her. The girls are heard speaking with an adult male in a foreign language. On several instances, the adult male's hand is seen in the video pushing and instructing the child who is performing the oral sex, and at one point pushes her head down and closer to the other child's vagina.

29. The second example, a 39-second video (file: 8358a709-85de-4f0b-b8b6-72b2c2bd0de4.mp4), depicts a girl, estimated to be approximately five to seven years old, performing oral sex on an adult male. The child appears to be kneeling while the adult male is sitting. She has brown hair and is wearing a green top. At one point in the video, the adult male asks the child to open her mouth and it is full of what appears to be semen.

30. A query of the NCMEC Database for other reporting related to the subject identifiers yielded three additional CyberTipline Reports, as detailed below.

31. On March 13, 2021, Snapchat submitted CyberTipline Report 87593609 to NCMEC. The report identified three images depicting suspected child pornography uploaded by an account associated with telephone number 7018184646; email address “jerrsmith85@gmail.com”; Screen/Username “jerry\_s1261”.

32. On April 21, 2021, Kik reported CyberTipline Report 89494766 to NCMEC. The report identified one image and 19 videos depicting suspected child pornography uploaded by an account associated with Screen/Username “doessizemater”; ESP User Identifier “doessizemater\_f9u” between 3/4/21 – 3/26/21.

33. On May 11, 2021, Snapchat submitted CyberTipline Report 90043116 to NCMEC. The report identified four images depicting suspected child pornography uploaded by an account associated with telephone number 7018184646; Screen/Username “smithr3764”.

#### **Premises, Person, and Vehicle Search Warrant**

34. On June 9, 2021, the Honorable Mustafa T. Kasubhai signed a search warrant authorizing the search of Cook’s residence; two vehicles—a blue semi-truck used by Cook for logging which displays his initials, “RLC,” and a Ford truck; and Cook’s person for evidence of violations related to child pornography. The warrant included “computers, storage media, or digital devices used as a means to commit the violations described above, including accessing and viewing child pornography.”

35. On June 11, 2021, law enforcement executed the search of Cook's residence. A number of digital devices were seized including three tablets, one external hard drive, and one laptop. A receipt for property was provided and the items seized were brought back to the FBI Eugene Resident Agency where they were entered into secure evidence storage and assigned item numbers 1B1, 1B2, 1B3, 1B4, and 1B5.

36. Also, on the morning of June 11, 2022, law enforcement located Cook in Lowell, Oregon. A traffic stop was conducted by Lane County Sheriff's Office deputies. Cook was driving a semi-truck bearing Oregon license plate YCDF371. This vehicle had not previously been identified by law enforcement as being operated by Cook. Cook's person was searched and no items were seized. After consultation with the United States Attorney's Office, the truck Cook was driving at the time of contact was searched pursuant to the motor vehicle exception.

37. During the search of that truck, Agents located two cell phones, a black OnePlus cell phone, IMEI 869904040440888 and a blue Samsung Galaxy S9, FCCID #A3LSMG96OU, the Subject Phone. Cook was informed that he was not under arrest but was advised of his rights and signed an FBI FD-395 consenting to speak with agents. During this interview Cook confirmed the two phones in the vehicle were his. Cook told agents the Black OnePlus phone found on the seat was his new phone. The Subject Phone that is the subject of this application, a Samsung Galaxy S9, was in a case and Cook identified it as his old phone. Cook provided the password for the Subject Phone and advised the Black OnePlus swipes up to unlock.

38. Both phones were seized, and a receipt for property was provided to Cook. The phones were brought back to the FBI Eugene Resident Agency where they were entered into

secure evidence storage and assigned item numbers 1B6 and 1B7. These items were maintained along with other items seized pursuant to the search warrant. Items 1B1, 1B2, 1B3, 1B4, and 1B5 have since been returned to their owner, another adult resident of the residence searched. The Subject Phone has remained in FBI custody since it was seized. Cook has not requested the return of the Subject Phone.

**Additional Information for the Court**

39. The following information is included to inform the Court; it is not being provided as part of the probable cause to support the warrant and I ask that the Court not consider it for that purpose. On June 11, 2021, the Subject Phone was searched and a Cellebrite extraction was conducted on the blue Samsung Galaxy S9, the Subject Phone, which is evidence item 1B7 in this matter. This extraction was subsequently transferred to a thumb drive and entered into evidence as item 1B9. I am aware of the results of that search. The evidence has been stored securely since such time in the Evidence Control Room at the FBI Eugene Resident Agency, located at 221 East 7th Avenue, Suite 320, Eugene Oregon 97401.

40. At the time the Subject Phone was searched, agents were acting under the belief that the search of the Subject Phone was authorized under the June 9, 2021 search warrant. It was later determined that the search of the truck, pursuant to the motor vehicle exception, was potentially an intervening factor and a separate warrant is likely appropriate. Your affiant is applying for such search warrant at this time.

### **Background on Digital Devices and Child Pornography**

41. Based on my knowledge, training, experience and the experience and training of other law enforcement officers with whom I have discussed the matter, I know that computers, computer technology, and the Internet have drastically changed the manner in which child pornography is produced and distributed.

42. Computers and Modern Smart Phones and other internet connected devices (hereinafter referred to as “digital devices”) serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

43. A digital device’s ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media used in digital devices has grown tremendously within the last several years. Many commercially available, relatively inexpensive drives can store over a million images at very high resolution. Images and videos of child pornography can also be stored on removable data storage media, such as external hard drives, thumb drives, media cards, and the like, many of which are small and highly portable and easily concealed, including on one’s person or one’s vehicle.

44. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion, including Internet Relay Chat, instant messaging programs, bulletin board services, e-mail, and “peer-to-peer” (P2P) file sharing programs. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Yahoo!, Hotmail, Google, Mega.nz, and Dropbox among others. The online services allow a



user to set up an account with a remote computing service that provides e mail or messaging services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any digital device with access to the Internet. Evidence of such online storage of child pornography is often found on the user's digital devices.

45. Communications made from a digital device are often saved or stored on that device and are shared among devices with shared cloud storage abilities such as iCloud or Google. Storage of information can be intentional, for example, by saving an e mail as a file on the device or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, digital device user's Internet activities generally leave traces in the computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a digital device contains P2P software, when the device was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data or deleted intentionally by the user.

### **Electronic Records**

46. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Subject Phone was used, the purpose of their use, who used them, and when. There is probable cause to believe

that this forensic electronic evidence will be on the Subject Phone because, based on my knowledge, training, experience, and information from other law enforcement agent I know:

a. Phones can store information for long periods of time, including information viewed via the Internet. Files or remnants of files can be recovered with forensic tools months or even years after they have been downloaded onto a phone, deleted, or viewed via the Internet. Electronic files downloaded to a phone can be stored for years at little or no cost. When a person “deletes” a file, the data contained in the file does not actually disappear, rather that data remains on the phone until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the phone that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, the operating system may also keep a record of deleted data.

b. Wholly apart from user-generated files, the Subject Phone may contain electronic evidence of how it has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, and file system data structures.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

d. Data on the Subject Phone can provide evidence of a file that was once on the Subject Phone but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Systems can leave traces of information on the Subject Phone that show what tasks and processes were recently active.

Web browsers, email programs, and chat programs store configuration information on the Subject Phone that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, including SD cards or other flash media, and the times the Subject Phone was in use. File systems can record information about the dates files were created and the sequence in which they were created.

e. Forensic evidence on a digital device can also indicate who has used or controlled it. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such “timeline” information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This “timeline” information may tend to either inculcate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user’s state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user’s motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a “wiping program” to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to

conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

f. A person with appropriate familiarity with how the Subject Phone works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how the Subject Phone was used, the purpose of their use, who used them, and when.

g. The process of identifying the electronically stored information necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on the Subject Phone is evidence may depend on other information stored on the Subject Phone and the application of knowledge about how a Phone functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

h. I know that when an individual uses a digital device to commit a crime such as to search, download, store and share child pornography, the individual's digital device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain: data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was

achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

i. Further, in order to find evidence of how the Subject Phone was used, the purpose of its use, who used it, and when, the examiner may have to establish that a particular thing is not present on the Subject Phone.

#### **Nature of examination**

47. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Subject Phone consistent with the warrant. The examination may require authorities to employ techniques, including imaging the Subject Phone and computer-assisted scans and searches of the entire Phone that might expose many parts of the devices to human inspection in order to determine whether it constitutes evidence as described by the warrant.

48. The initial examination of the Subject Phone will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

49. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Subject Phone or image do not contain any data falling

within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

50. If an examination is conducted, and it is determined that the Subject Phone does not contain any data falling within the ambit of the warrant, the government will return the Subject Phone to its owner within a reasonable period of time following the search and will seal any images of the Subject Phones, absent further authorization from the Court.

51. If the Subject Phone contains evidence, fruits, contraband, or is an instrumentality of the crime, the government may retain the Subject Phone as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Subject Phone and/or the data contained therein.

52. The government will retain a forensic image of the Subject Phone for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

53. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve

the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

### **Conclusion**

54. Based on the foregoing, I submit that probable cause exists to believe, and I do believe, that the Subject Phone described in Attachment A contains evidence of violations of Title 18, United States Code, Sections 2252A(a)(2), (b)(1) and 2252A(a)(5)(B) and (b)(2), as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the Subject Phone described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

55. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) William McLaren, and AUSA McLaren advised that, in his opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

### **Request for Sealing**

56. It is respectfully requested that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrant, including the application, this affidavit, the attachments, and the requested search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time may cause flight from prosecution, cause destruction of or tampering with evidence, cause intimidation of potential

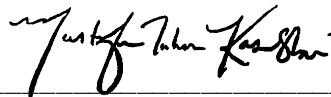
witnesses, or otherwise seriously jeopardize an investigation. Premature disclosure of the contents of the application, this affidavit, the attachments, and the requested search warrant may adversely affect the integrity of the investigation.

/s/ Deane Davis per rule 4.1

---

DEANE DAVIS  
Special Agent, FBI

Subscribed and sworn to before me telephonically pursuant to FRCP 4.1 this 28  
day of October 2022 at 4:45pm./p.m. in the District of Oregon.



---

MUSTAFA T. KASUBHAI  
United States Magistrate Judge



## **ATTACHMENT A**

### **Phone to Be Searched**

The Subject Phone to be searched is a blue Samsung Galaxy S9, FCCID #A3LSMG96OU, currently in FBI Secure Evidence Storage and assigned item number 1B7. The search will take place in the Eugene, Oregon office of the FBI, at 211 E. 7th Ave, Suite 320, Eugene, OR 97401.

## **ATTACHMENT B**

### **Items to Be Seized**

1. All records on the Subject Phone described in Attachment A that relate to violations of Title 18, United States Code, Section 2252A, involving the transportation, distribution, receipt, and possession of child pornography, that involve Randy Lee Cook, since May 28, 2020, including:

a. Any and all records, documents, or materials, including correspondence, that pertain to the production, possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

b. All originals and copies of visual depictions of minors engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

c. Any and all motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256, video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

d. Any and all records, documents, or materials which include offers to transmit, through interstate commerce by any means, any visual depiction of a minor engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

e. Any and all records, documents, or materials relating to the production,

reproduction, receipt, shipment, trades, purchases, or transactions of any kind involving the transmission, through interstate commerce, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

f. Any and all records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

g. Any records of Internet usage, including records containing screen names, usernames, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, and e-mail messages.

2. Evidence of user attribution showing who used or owned the Phone at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the Internet, including:

a. Records of Internet Protocol addresses used.

b. Records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

c. Records of data storage accounts and use of data storage accounts.

4. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or

stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

### **Search Procedure**

5. The examination of the Phone may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Phone to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the Phone will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Phone or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the Phone does not contain any data falling within the ambit of the warrant, the government will return the Phone to its owner within a reasonable period of time following the search and will seal any image of the Phone, absent further authorization from the Court.

9. If the Phone contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Phone as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Phone and/or the data contained therein.

10. The government will retain a forensic image of the Phone for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.